

7. *Measures to ensure information accuracy.* If the system is to be used to make determinations about the rights, benefits, or entitlements of individuals, describe the measures being established to ensure the accuracy, currency, relevance, and completeness of the information used for these purposes.

8. *Other measures to ensure system security.* Describe the steps taken to minimize the risk of unauthorized access to the system. A more detailed assessment of security risks and specific administrative, technical, and physical safeguards will be available for review upon request.

9. *Relationship to state and local government activities.* Describe the relationship of the system to state or local government activities that are the sources, recipients, or users of the information in the system.

C. *Supporting Documentation.* Item 10 of the narrative is captioned *Supporting Documents*. A positive statement for this caption is essential for those enclosures that are not required to be enclosed. For example, “No changes to the existing DLA procedural or exemption rules (32 CFR part 323) are required for this proposed system.” List in numerical sequence only those enclosures that are actually furnished. The following are typical enclosures that may be required:

1. For a new system, an advance copy of the system notice which is proposed for publication; for an altered system an advance copy of the notice reflecting the specific changes proposed.

2. An advance copy of any proposed exemption rule if the new or altered system is to be exempted. If there is no exemption, so state in the narrative.

3. Any other supporting documentation that may be pertinent or helpful in understanding the need for the system or clarifying its intended use. While not required, such documentation, when available, is helpful in evaluating the new or altered system.

[DLAR 5400.21, 51 FR 33595, Sept. 22, 1986. Redesignated and amended at 56 FR 57803, Nov. 14, 1991]

APPENDIX D TO PART 323—WORD PROCESSING CENTER (WPC) SAFEGUARDS

A. *Minimum Standards of Protection.* All personal data processed using word processing equipment will be afforded the standards of protection required by this regulation. The special considerations discussed in this enclosure are primarily for Word Processing Centers (WPCs) operating independent of the customer's function. However, managers of word processing systems are encouraged to consider and adopt, when appropriate, the special considerations described. WPCs that are not independent of a customer's function are not required to prepare formal written risk assessments.

B. *WPC Information Flow.* In analyzing procedures required to safeguard adequately personal information in a WPC, the basic elements of WPC information flow and control must be considered. These are: Information receipt, information processing, information return, information storage and filing. WPCs do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

C. *Safeguarding Information During Receipt.*

1. The word processing manager will establish procedures:

a. That require each customer who requests that information subject to this DLAR be processed to identify specifically that information to the WPC personnel. This may be done by:

(1) Providing a check-off type entry on the WPC work requests.

(2) Requiring that the WPC work requests be stamped with a special legend, or that a special notation be made on the work requests.

(3) Predesignating specifically a class of documents as coming within the provisions of this DLAR (such as, all officer effectiveness reports, all recall rosters, and all medical protocols).

(4) Using a special cover sheet both to alert the WPC personnel as to the type information, and to protect the document during transmittal.

(5) Requiring an oral warning on all dictation.

(6) Any other procedures that ensure the WPC personnel are alerted to the fact that personal data subject to this DLAR is to be processed.

b. To ensure that the operators or other WPC personnel who receive data for processing not identified as being under the provisions of this DLAR, but that appear to be personal, promptly call the information to the attention of the WPC supervisor or the customer.

c. To ensure that any request for the processing of personal data which the customer has not identified as being in a system of record, and that appears to meet the criteria set forth in this regulation, is called to the attention of the appropriate supervisory personnel and system manager.

2. The WPC supervisor will ensure that personal information is not inadvertently compromised within the WPC.

D. *Safeguarding Information During Processing.* 1. Each WPC supervisor will establish internal safeguards that will protect personal data from compromise while it is being processed.

2. Physical safeguards may include:

a. Controls on individual access to the center.

b. Machine configurations that reduce external access to the information being processed, or arrangements that alert the operator to the presence of others.

c. Using certain specific machines to process personal data.

d. Any other physical safeguards, to include special technical arrangements that will protect the data during processing.

3. Other safeguards may include:

a. Using only certain selected operators to process personal data.

b. Processing personal data only at certain times during the day without the WPC manager's specific authorization.

c. Using only certain tapes or diskettes to process and store personal data.

d. Using continuous tapes for dictation of personal data.

e. Requiring all WPC copies of documents to be marked specifically so as to prevent inadvertent compromise.

f. Returning extra copies and mistakes to the customer with the product.

g. Disposing of waste containing personal data in a special manner.

h. Any other local procedures that provide adequate protection to the data being processed.

E. *Safeguarding Information During Return.* The WPC shall protect the data until it is returned to the customer or is placed into a formal distribution channel. In conjunction with the appropriate administrative support personnel and the WPC customers, the WPC manager will establish procedures that protect the information from the time word processing is completed until it is returned to the customer. Safeguarding procedures may include:

1. Releasing products only to specifically identified individuals.

2. Using sealed envelopes to transmit products to the customer.

3. Using special cover sheets to protect products similar to the one discussed in above.

4. Hand-carrying products to the customers.

5. Using special messengers to return the products.

6. Any other procedures that adequately protect products from compromise while they are awaiting return or being returned to the customer.

F. *Safeguards During Storage.* The WPC manager shall ensure that all personal data retained in the center for any purpose (including samples) are protected properly. Safeguarding procedures may include:

1. Marking will hard copies retained with special legends or designators.

2. Storing media containing personal data in separate files or areas.

3. Marking the storage containers for media containing personal data with special legends or notations.

4. Restricting the reuse of media used to process personal data or erasing the media before reuse.

5. Establishing special criteria for the WPC retention of media used to store and process personal data.

6. Returning the media to the customer for retention with the file copies of the finished products.

7. Discouraging, when practical, the long-term storage of personal data in any form within the WPC.

8. Any other filing or storage procedures that safeguard adequately any personal information retained or filed within the WPC.

G. *Risk Assessment for WPCs.* 1. Each WPC manager will ensure that a formal, written risk assessment is prepared for each WPC that processes personal information subject to this regulation. The assessment will address the areas discussed in this enclosure, as well as any special risks that the WPC location, configuration, or organization may present to the compromise or alteration of personal data being processed or stored.

2. A risk assessment will be conducted at least every 5 years or whenever there is a change of equipment, equipment configuration, WPC location, WPC configuration or modification of the WPC facilities that either increases or decreases the likelihood or compromise of personal data.

3. Copies of the risk assessment will be retained by the WPC manager and made available to appropriate inspectors, as well as to personnel studying equipment for facility upgrading of personal data.

H. *Special Considerations in WPC Design and Modification.* Procedures will be established to ensure that all personnel involved in the design of WPCs or the acquisition of word processing equipment are aware of the special considerations required when processing personal data subject to this DLAR.

APPENDIX E TO PART 323—OMB GUIDELINES FOR MATCHING PROGRAMS

A. *Purpose.* These guidelines supplement and will be used in conjunction with OMB Guidelines on the Administration of the Privacy Act of 1974, issued on July 1, 1975, and supplemented on November 21, 1975. They replace earlier guidance on conducting computerized matching programs issued on March 30, 1979. They are intended to help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching. They are designed to address the concern expressed by the Congress in the Privacy Act of 1974 that "the increasing use of computers and sophisticated information technology, while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or